Information Operations as a Deterrent to Armed Conflict

Colonel Blane R. Clark, U.S. Army, Retired

We must hold our minds alert and receptive to the application of unglimpsed methods and weapons.

—General Douglas A. MacArthur

INFORMATION OPERATIONS (IO) provide the commander with nonlethal, flexible deterrent options. Applying IO this way is viable for both state and nonstate adversaries. The greatest impact will vary depending on the particular core capability the adversary has. Information operations core capabilities have the most significant strategic effect as a deterrent to conflict when applied during phase I of Joint operations. Indeed, the central strategic aim of IO is to deter threats of potential adversaries.[1] Information operations-induced deterrence compels an adversary to adopt a policy or take an action that obtains or sustains the national security of U.S. interests. Applications of IO at the strategic level have essentially consisted of only one or two core capabilities as tactical enablers rather than synergistic combinations for a strategic effect.

Information operations planned, integrated, and executed as part of a combatant command's campaign plan during phase I provide the commander with nonkinetic, nonlethal options to achieve strategic objectives. The probability of effectiveness in phase I rises when commanders integrate IO into deliberate and crisis action planning cycles. Such integration should occur from inception and be included in rigorous Joint targeting processes. Measures of effectiveness must be developed to inform any decisions to re-engage or terminate IO actions.

Applying concentrated, integrated, and synchronized IO to deter an adversary from a course of action and preclude an outbreak of armed conflict does not constitute an act of war.[2] However, though not an act of war, it does involve targeting. If the application of IO is to achieve the desired deterrent effect, three enabling components must align—the capabilities to engage a target, access to the target, and the authority to engage the target.

Colonel Blane R. Clark, U.S. Army, Retired, served as the chief, Information Operations Division, J3, U.S. Central Command, from January 2005 to June 2008 and as director, C4 and Information Operations, and as an instructor at the U.S. Army War College from July 2008 to December 2009. He holds an M.S. from the University of Southern California.He has served in command and staff positions in the continental United States, Korea, Germany, and Iraq. COL Clark is currently the vice J3, Joint Task Force-Global Network Operations (JTF-GNO) and assistant deputy for Current Operations (J33) for the consolidated Joint Functional Component Command–Network Warfare/JTF-GNO at Ft. Meade, MD.

PHOTO: U.S. Army Soldiers assigned to 213th Psychological Operations Company observe a reaction after playing an announcement over a loud speaker out of Joint Security Station Oubaidy located just outside Sadr City, Iraq, after a series of rocket and mortar attacks, 29 March 2008. (U.S. Air Force, SSGT Jason T. Bailey)

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
JUN 2010		**00-05-2010 to 00-06-2010**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Information Operations as a Deterrent to Armed Conflict	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **U.S. Army Combined Arms Center,Fort Leavenworth,KS,66027**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**Same as Report (SAR)**	**8**	

Foundations for Information Operations

Information operations core military capabilities include electronic warfare, computer network operations, psychological operations, military deception, and operations security. When properly coordinated and closely focused, these capabilities can deter armed conflict. Information operations' primary goal at the strategic level is to coerce a key leader or group of leaders to forgo a particular action or, alternatively, take an action consistent with U.S. interests.[3]

Information operations are not the application of any of the core capabilities singularly. The synchronized and coordinated integration of combinations of the core capabilities characterizes information operations, and this generates the offensive nonkinetic force component that can deter armed conflict.

Electronic warfare. This core capability is comprised of the three subdivisions—electronic attack, electronic protection, and electronic support. These all represent military action during which electromagnetic or directed energy weapons control the electromagnetic spectrum or attack an enemy.[4] Because the focus is on deterrence, electronic attack has the most direct relevance.

Electronic attack targets enemy facilities, equipment, or personnel to degrade, neutralize and, if necessary, destroy an enemy's electronic support systems.[5] As an example, electronic attack airborne assets could conduct standoff communications jamming against an enemy's integrated air defense system communications network so that the enemy suffers a degradation of its system's command and control capability.

Computer network operations. The latest IO core capability integrated into Joint Publication 3-13, *Computer Network Operations*, has three subcomponents—computer network attack, computer network defense, and computer network exploitation.[6] Again, since the focus is on causing a deterrent effect, the offensive computer network attack represents the most viable "effects generating" subcomponent.

Computer network attack involves using computer networks to deny, disrupt, or degrade computers, computer networks, or the information resident in any of those. Today, potential adversary groups rely more and more on computers and computer networks to facilitate command and control, support enabling transactions, and coordinate actions.[7]

Computer network attack has the potential to be a weapon of mass disruption against both military and civilian infrastructure targets.[8] As an example, an Internet denial-of-service attack consisting of the injection of a large stream of data against an adversary computer network has the potential to consume all available bandwidth on that network and significantly degrade or deny its use.

Psychological operations. This core capability involves delivering information that influences or dissuades key adversary leadership and their support structures so that follow-on adverse actions by the adversary are deterred. Psychological operations are most effectively employed as an integrated IO capability in support of phase I operations.[9] Psychological operations influence foreign populations and counter adversary messages.[10] Messages broadcast via shortwave radio, warning the general population that the actions of their leaders may result in military action, are an example. Within the Department of Defense, only psychological operations forces have the authority to influence foreign target audiences using an array of radio, print, and other associated media delivery mechanisms.[11]

Military deception. This core capability deliberately targets key adversary decision makers to mislead them into making a decision favorable to friendly objectives. As a weapon for deterrence, it causes doubt, confusion, and possibly fear among key adversary leadership targets by disrupting or degrading their normal command and control decision cycle as it wrestles to evaluate the deception.[12] A message targeted to exploit a fissure between a key member of the adversary's leadership who has a contentious relationship with another key decision maker is an example. That message could cause internal strife resulting in the adversary foregoing an intended course of action and adopting a position more favorable to our interests.

Operations security. In phase I, operations security denies the adversary critical information that would facilitate an accurate assessment of our intent and capabilities. In addition, effective operations security causes the adversary either to make erroneous decisions or to delay decisions due a lack of credible information.[13]

Denying the adversary decision maker critical information about our intent and capabilities contributes to his uncertainty, disrupts his decision cycle, and escalates his mounting sense of doubt, fear and confusion, which makes deterrence a real possibility.[14]

Five additional capabilities support IO—counterintelligence, physical security, information assurance, combat camera, and physical attack. Except for physical attack, these measures act to defend friendly infrastructure or visual information documentation and are not as germane to achieving deterrence. Physical attack involves the use of kinetic fires against an information operations target to influence a specific target audience.[15]

While doctrine states that the three IO-related capabilities of public affairs, civil-military operations, and defense support to public diplomacy contribute to the overall information environment and must be coordinated with IO, arguably their application as related to offensive information operations to achieve deterrence is indirect at best. Military IO targets the adversary and the adversary's support structures. Public affairs operations convey messages to domestic and foreign audiences. Civil military operations are most effective in phase IV (stabilize) and V (enable civil authority) operations. Defense support to public diplomacy equates to psychological operations-trained Soldiers supporting dissemination of messages and themes under the authority of an ambassador. These related capabilities are not as effective as IO capabilities in terms of achieving deterrence in phase I.[16]

Information Operations in Phase I: A Compelling Position

Undergirded by committed political will, IO offers combatant commanders a nonlethal option that, when applied within the context of an overall set of strategic objectives, can deter conflict. Indeed, the primary strategic emphasis of IO should be deterrence and the employment of core capabilities toward that end.[17] For IO to be effective in deterring a potential adversary, we must apply them with the same force and rigor that characterize our application of lethal force. We must leave our adversary with an overwhelming sense that pursuing a course of action that the United States deems as threatening to U.S. national interests is fruitless, and that the continued pursuit of that course of action brings dire consequences. Information operations applied effectively in support of deterrence leave the adversary with a sense of doubt, fear, and confusion and influences him to abandon a course of action. With IO orchestrated to influence the adversary's observe-orient-decide-act ("OODA") loop, his operations and perception of the possibility of success diminish. This creates the real possibility that the adversary may abandon or alter the policy challenged by the United States.[18]

The value of applying IO to deter conflict has widely recognized appeal. In the *National Security Strategy of the United States*, deterring a potential adversary is one of the top priorities for securing U.S. national interests.[19] The document speaks directly to the need to engage a potential adversary with the capabilities of IO before the onset of armed conflict.

Interestingly, the *National Security Strategy* also points to "dissuading" as a top priority for securing U.S. interests.[20] Dissuading involves those activities associated with phase 0 (shaping operations). In phase 0, military IO should play a minor role only. Other elements of national power—diplomatic, informational, and economic—should dominate U.S. efforts to dissuade an adversary from pursuing a policy that threatens U.S. security interests.

The distinction between dissuading and deterring a potential adversary resides with the focus of force. With dissuading efforts, the focus often takes a less direct approach to the adversary. In contrast, deterrence requires directed pressure against a potential adversary. The targets for the application of deterrent IO must correspond directly to the critical human, infrastructural, and content components that sustain the potential adversary and the policy or course of action he is pursuing.

…the *National Security Strategy* also points to "dissuading" as a top priority…

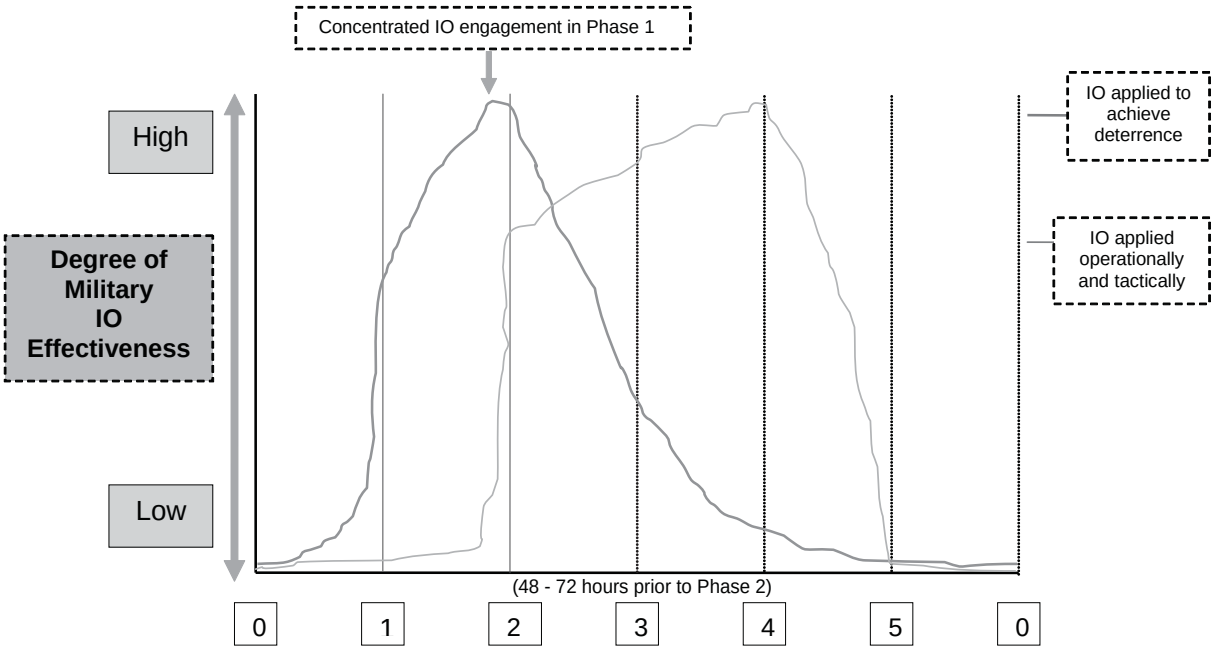

Figure 1. Information operations in phase I, deterrence.

Department of Defense Directive 3600.1 addresses IO and endorses the need to leverage IO capabilities to achieve deterrence. The directive states that IO should aim to deter conflict and that the potential to defuse a crisis is its greatest promise.[21] Phase 0 constitutes the shaping phase of Joint operations and phase II, the "seize the initiative" phase, represents the onset of armed conflict. Information operations quickly devolve to tactical application as they are applied offensively in phase II. In phase I, IO fills the strategic deterrence gap between dissuading in phase 0 and the onset of lethal force in phase II. The more aggressive the use of IO in phase I, the more likely the adversary will perceive our willingness to use force.[22] Information operations in support of strategic deterrence can thereby minimize the requirement for forward deployed and stationed forces.[23] Information operations will influence the decision making and perceptions of a potential adversary while increasing the deterrent impact of power-projection options.[24]

Figure 1 portrays the deterrent effectiveness of information operations across the phases of Joint operations. Analysis of this diagram will further clarify the compelling argument for offensive IO in phase I operations along with a concentrated IO engagement as phase I approaches culmination and phase II is about to begin.

The line to the left represents IO applied to achieve deterrence. The diagram shows that IO effectiveness is minimal in phase 0, but rapidly accelerates with the onset of phase I and increases across phase I in an accumulating manner. This increasing effectiveness reflects that the potential adversary is reacting to the synchronized application of the core military information operations capabilities. In phase I, IO should aim to affect an adversary's leadership and its supporting structures, to include populations, to such an extent that the U.S. achieves its goal to deter conflict by compelling the favorable change of an adversary policy.[25] As the onset of phase II approaches, the diagram illustrates that a concentrated IO engagement needs to occur that ensures, first, successful deterrence and, failing deterrence, friendly forces information superiority in preparation for the onset of armed conflict in phase II. The central characteristic of the concentrated IO engagement is a redoubling of effort and a massing of IO "fires." Should deterrence fail, the concentrated IO engagement in phase I should begin within 48 to 72 hours of the anticipated commencement of

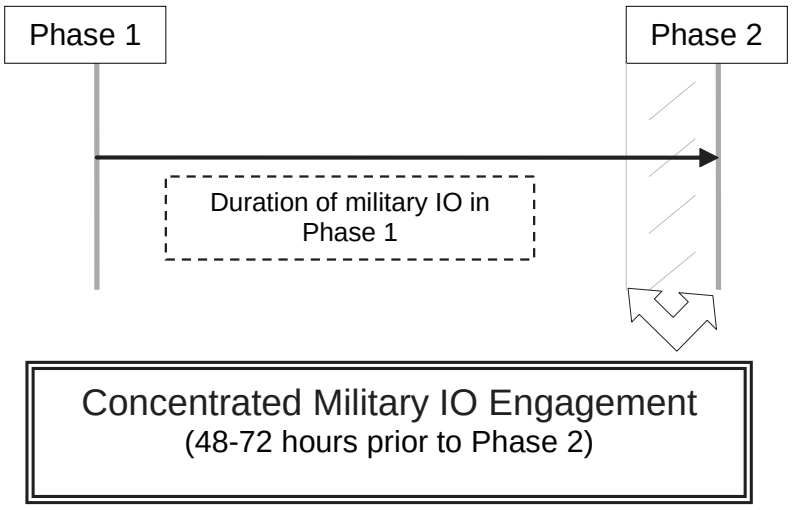

Figure 2. Information operations across a phase I timeline.

phase II. Figure 2 depicts the timeline for initiating and executing the concentrated IO engagement in phase I.

As phase II commences, the strategic impact of IO as an option to achieve deterrence quickly becomes subservient to the application of IO in support of operational and tactical demands.

The same assets used in phase I for IO also support the operational and tactical fight, and their application increases from the onset of phase II through the culmination of phase III, main combat operations. At the onset of phase VI, stability operations, operational and tactical IO decline in effectiveness.

An aggressive, synchronized, and coordinated application of the five core capabilities to deter the actions of a potential state adversary may be as follows:

- Electronic warfare may target the adversary's ballistic missile command and control network and the associated radars to degrade delivery capability. It may jam state-owned radio and television stations to isolate the population from further state propaganda.
- A computer network attack against the state-controlled telecommunications network can deny, degrade, or disrupt its use for command and control of military forces and for use by key leadership to direct a national response. Such an attack, in conjunction with psychological operations, can deliver discreet messages to key leaders of factional groups to create friction and increase internal pressure on the adversary state leadership to abandon its contentious policies.
- Psychological operations can deliver broadcast messages to the population in order to create separation from the adversary state leadership and add additional internal pressure.
- Military deception operations can cause the key military leadership doubt, fear, and confusion as to legitimate U.S. military intentions. These operations will compel the adversary state military leaders to confront the political leadership with the futility of resistance.
- Operational security can surround the operations of friendly forces with a blanket of security and thwart the detection of U.S. intentions.

The combatant commander seeks to isolate the leaders of a potential adversary from the physical and psychological support they enjoy, especially from their military forces and supporting infrastructure.[26] If the actor is a nation-state, dependence on a more formalized bureaucracy and embedded technology, such as telecommunications networks and radar networks, will probably be greater than that of a nonstate actor. Therefore, electronic warfare and computer network attacks may have a greater effect against a state actor than a nonstate actor may.

…application of offensive IO can diffuse a crisis…

In either case, the application of offensive IO can diffuse a crisis and preclude the need to move into the armed conflict stage that begins with phase II.[27]

The lack of technological sophistication and less formalized command and control of typical potential nonstate adversaries, as compared to state adversaries, may well limit the direct effectiveness of electronic warfare and computer network attack. However, since nonstate adversaries may use the telecommunications infrastructure of the host country in which they operate, computer network attack has the potential to work as an enabling capability for the delivery of direct psychological operations messages. Likewise, computer network attacks can enable psychological operations messages to key leaders of the host country, encouraging bolder action against the adversary.

Influence operations using psychological operations and military deception will have the greatest impact on an adversary that lacks technological sophistication for command and control. Military deception can cause the leadership of the nonstate adversary to become suspicious of the host nation's further tolerance of its activities and create fear as to pending military operations against them by U.S. lead coalition forces. Psychological operations against the local population can erode support for the adversary. For example, offering a reward for information entices the local population to report the activities of the adversary group.

Both scenarios demonstrate that successful application of military information operations against any potential adversary requires the following:

- Analysis of the environment to ensure the proper synchronization of core capabilities.
- Assessment of the vital interests of the potential adversary to ensure that the planning for information operations is on target.
- Assessment of a potential adversary's critical pressure points to ensure that the force applied by information operations achieves maximum effectiveness.
- Use of the appropriate information operations capability, or capabilities, in the degree and range of force necessary to achieve the desired deterrent effect.[28]

Planning, Targeting, and Effectiveness

Information operations should integrate fully into planning and targeting, and measures of effectiveness should provide the feedback to insure its effectiveness. Key to effectiveness is the use of all synchronized and integrated core capabilities.[29] Effectiveness in phase I operations is doubtful unless IO is integrated into planning and targeting. Information operations planners must participate as active members in established operations planning teams and stand ready to defend the value of IO products as both a unique set of capabilities and as a force multiplier across all phases of Joint operations.[30]

Using traditional targeting procedures is necessary and appropriate because information operations provide effects-producing options, just as lethal options do. A targeting synchronization matrix depicting integration of targets is as applicable for information operations as it is for lethal capabilities.[31] There should be only one target synchronization matrix that integrates lethal and nonlethal targets. Measures of effectiveness should be logically linked to a desired end state. However, one must recognize that measures of effectiveness are a tremendous challenge. The cumulative effect of information operations that is necessary to achieve deterrence makes the impact of each individual capability difficult to assess.[32]

Arguably, a measure of effectiveness for each core capability is irrelevant when the synchronization of two or more capabilities is needed to achieve a desired effect. Without a measure of effectiveness based on deductive analysis for first-order effects and reasonable inductive analysis for second- and third-order effects, the acceptability of information operations as a set of predictable nonlethal options for the commander is specious.

Legal and Moral Justification

Armed conflict is governed by international law.[33] Information operations fall outside this legal framework. International law does not mention use

...information operations accommodate efforts to adhere to traditional moral and legal restrictions...

of information operations as an aspect of armed conflict, so use of IO as a deterrent to war does not constitute an act of war.[34]

Article 41 of the UN Charter is one example of current governing bodies of law that do not categorize the use of information operations as an act of war. It states that acts to interrupt the communications of an adversary do not involve the use of armed force.[35] Therefore, the use of information operations in deterrence operations, such as electronic warfare and computer network attack, do not constitute an act of war.

Within the context of the Laws of Armed Conflict, the conditions of *jus in bello,* how a force is used in war, involves principles of necessity, proportionality, discrimination, and humanity. The Geneva and Hague conventions codify the conditions for *jus in bello*. These conventions do not contain any specific control agreements that limit the use of information operations.[36] In fact, information operations accommodate efforts to adhere to traditional moral and legal restrictions meant to encourage restraint and minimize the use of force.[37] For instance, the principle of proportionality requires that the value of a military objective balance against the loss of life and damage caused by a military action.[38] Information operations help meet the demands to satisfy this principle. The principle of discrimination likewise requires that targets attacked have a military value and not be solely civilian in nature.[39] Since the capabilities of information operations do not directly cause loss of life or infrastructure damage, and arguably neither do possible second- and third-order effects, the mandate of this principle is met. Likewise "humanity" as a principle of *jus in bello* requires the mitigation of human suffering in war.[40] Here again, information operations can lead to more moral outcomes.

Conclusion

The core military information operations capabilities can deter armed conflict with both state and nonstate potential adversaries. The results of actions the U.S. takes to deter a potential adversary from an undesirable course of action or policy, and not the weapons used, will constitute how the international community and domestic audience judge the United States.[41] The ability to justify the use of offensive IO as morally prudent will significantly contribute to the acceptance by the international community that the use of IO does not constitute the use of force in the classic sense.[42]

Today, U.S. policy and military leaders tend to adhere to an operational constraint that seeks to minimize casualties, especially for U.S. forces and the affected civilian population base.[43] Clearly, IO with nonlethal, nonkinetic characteristics meet this operational constraint and offer justification for offensive information operations. The more the use of IO for deterrent purposes is understood, the more U.S. political and military leaders are likely to agree that military information operations offensively applied in phase I will achieve deterrence with minimal casualties and loss of infrastructure. Then, and only then, will the Nation embrace IO enough to allow its full contribution to national security as a deterrent.[44]

The application of information operations as a deterrent to armed conflict holds considerable promise for military and political leaders alike. However, the country currently lacks the political will and some enabling factors to permit offensive information operations as a phase I force option when seeking to achieve a strategic objective.

The following five enabling factors would support successful offensive IO in phase I. Accepted and implemented together, they provide real hope for progress.

- Expand doctrine in Joint Publications 3-0 and 3-13 to specify that the use of offensive information operations in phase I of Joint operations constitutes what amounts to a first option for the combatant commander. The doctrine could specify a concentrated information operations engagement as a culminating application in phase I, a last concerted effort to force a potential adversary to acquiesce to U.S. deterrent pressure or as a precursor for favorable phase II operations.

- Establish IO as a core capability in all combatant commands.[45] To do so requires additional new, technically superior IO weapons along with an adequate force structure to implement them. Too few assets, both in weapons and forces available, exist to support all combatant commands on anything approaching simultaneous engagements or to adequately mass IO "fires" in the quantity necessary to achieve effectiveness. Establishing a joint development and acquisition office chartered to explore, develop, and field technically superior IO weapon systems in sufficient quantities for application in air, land, and sea environments is necessary. A Joint force structure that provides each geographic combatant command, Special Operations Command, and U.S. Strategic Command with a direct support organization is also necessary. Each of these organizations could plan and execute information operations with organic capabilities assigned or attached.

- Address basic issues related to preparation of the battlespace to support offensive information operations in directives, policy, and doctrine.[46] A presidential directive to the intelligence community that directs proactive, aggressive intelligence preparation of the battlespace against all potential adversaries for the purpose of gaining access to that adversary's critical information nodes to support offensive IO is critically needed. The process for gaining access to a sensitive adversary IO target is too slow, too cumbersome, highly politicized, and favors intelligence process over operational necessity.

- Provide authority for combatant commanders to execute offensive information operations critical to ensuring that they are a force option for deterrence. A comprehensive policy should be established that directs that all existing information operations capabilities and supporting force structures be authorized for employment by a combatant commander in support of deterrent operations. Specific tests should establish the criteria that set the acceptable conditions for the use of information operations in phase I.

- Call for the U.S. government to use information operations to achieve strategic national objectives and protect national interests. Unless there is the political will to use IO in phase I to deter a potential adversary, armed conflict is probable, with its attendant casualties and expenditure of resources. ***MR***

NOTES

1. Joint Chiefs of Staff (JCS), Joint Publication (JP) 3-13, *Information Operations,* (Washington, DC: U.S. Government Printing Office [GPO], 13 February 2006), 1-12.
2. Earl E. Miller, Army Transformation and Information Operations: The International Legal Implications (Strategy Research Project, Carlisle Barracks, PA: U.S. Army War College, 9 April 2002), 8-9.
3. Leigh Armistead, ed. *Information Operations: Warfare and the Hard Reality of Soft Power* (Washington, DC: Brassey's Inc., 2004), 16.
4. JCS, Joint Publication 3-51, *Joint Doctrine for Electronic Warfare* (Washington, DC: GPO, 7 April 2000), vii.
5. Ibid., 1-2.
6. JCS, *Information Operations,* II-6.
7. Ibid.
8. Jennie M. Williamson, Information Operations: Computer Network Attack in the 21st Century (Strategy Research Project, Carlisle Barracks, PA: U.S. Army War College, 9 April 2002), 9.
9. JCS, JP 3-53, *Joint Doctrine for Psychological Warfare* (Washington, DC: GPO, 5 September 2003), ix.
10. Ibid., x.
11. Ibid., xii.
12. JCS, JP 3-58, *Joint Doctrine for Military Deception* (Washington, DC: GPO, 31 May 1996), v-vi.
13. JCS, JP 3-54, *Joint Doctrine for Operations Security* (Washington, DC: GPO, 24 January 1997), v-vi.
14. Ibid., I-4.
15. JCS, *Information Operations*, II-7–II-10.
16. JCS, *Information Operations*, II-10–II-13.
17. Roger W. Barnett, "Information Operations, Deterrence, and the Use of Force," *Naval War College Review* (Spring 1998): 1.
18. Paul R. Guevin, "Information Operations," *Air and Space Power Journal* 18, no. 2 (Summer 2004): 122.
19. Department of Defense (DOD) *The National Defense Strategy of the United States of America* (Washington, DC: GPO, March 2005), iv.
20. Ibid.
21. Brian E. Fredericks, "Information Warfare at the Crossroads," *Joint Force Quarterly* (Summer 1997): 100.
22. Ibid., 98.
23. DOD, *Joint Operations Concepts* (Washington, DC:GPO, November 2003), 19.
24. Arthur N. Tulak, "Information Operations in Support of Demonstrations and Shows of Force," *Military Intelligence Professional Bulletin* 29, no.3 (July-September 2003): 10.
25. David L. Grange and James A. Kelley, "Information Operations for the Ground Commander," *Military Review* (March-April 1997): 9.
26. JCS, JP 3-0, *Doctrine for Joint Operations* (Washington, DC: GPO, 10 September 2001), IV-2.
27. J.E. Rhodes, "A Concept for Information Operations," *Marine Corps Gazette* 82, no. 8 (August 1998): 48.
28. Leigh Armistead, ed., 21.
29. Dennis M. Murphy, "Information Operations on the Non-traditional Battlefield," *Military Review* (November-December 1996): 18.
30. Maryann Lawlor, "Information Operations Specialists Move to the Mission Planners' Table," *Signal* (December 2005): 47.
31. Richard L. Gonzales and Marc J. Romanych, "Nonlethal Targeting Revisited," *Field Artillery Journal* (May-June 2001): 6-8.
32. David C. Grohoski, Steven M. Seybert and Marc J. Romanych, "Measures of Effectiveness in the Information Environment," *Military Intelligence Professional Bulletin* 29, no. 3 (July-September 2003): 12-14.
33. David J. DiCenso, "Information Operations: An Act of War?" *Law Technology* 33, no. 2 (2d Quarter 2002): 28.
34. Miller, 14.
35. Ibid., 29.
36. Barnett, 6.
37. DiCenso, 31.
38. Ibid.
39. Ibid.
40. Ibid.
41. Miller, 11.
42. Barnett, 7.
43. Ibid., 5.
44. Ibid., 1.
45. Richard B. Myers, "Shift to a Global Perspective," *Naval War College Review* 56, no. 4 (Autumn 2003): 11.
46. Walter Jajko, "A Critical Commentary on the Department of Defense Authorities for Information Operations," *Comparative Strategy* 21 (2002): 111.